OSI 4.katman
(Transport - İletim layer)
Güvenliği

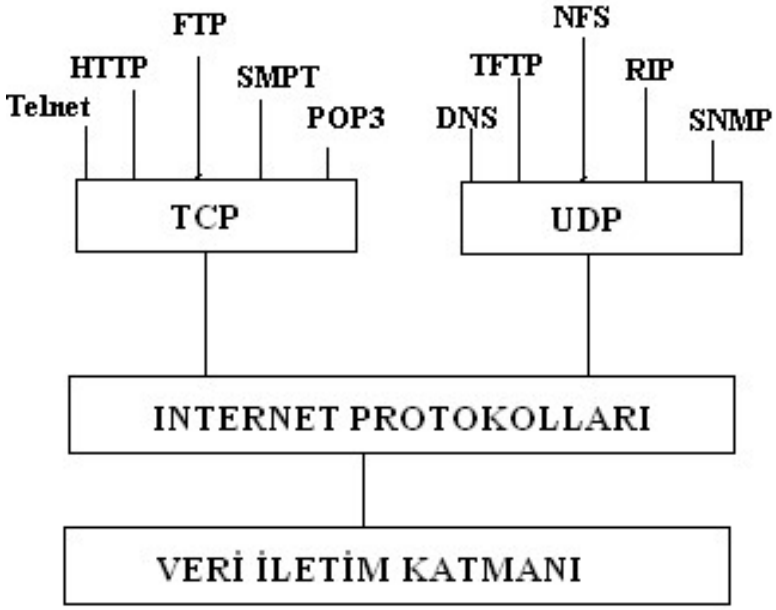
İletim katmanı protokolları

OSI modelinde, farklı ana sistemler üzerindeki uygulamalar arasındaki iletişimi sağlayan katman **transport** katmanıdır. Bu katman bünyesinde, TCP ve UDP gibi veri iletişimini farklı şekillerde sağlamak üzere iki protokol barındırır.

•**TCP (Transmission Control Protocol);** bağlantıda olan iki ucun senkonize olarak çalışmasını sağlar, hata denetimi yapar, güvenli veri akışını sağlar.

•**UDP(User datagram Protocol)** ise iletişim içinde olan iki nokta arasında senkronizasyon öngörmez, güvenilir olmayan veri akışı gerçekleştirir.

• Tek başına TCP ve UDP protokollerini kullanarak uzaktaki makinalara doğrudan veri iletimi yapılamaz. Fakat aynı bilgisayarda çalışan uygulamalar arasında veri iletişimi yapılır.



TCP protokolu, iki uç arasında bağlantıya dayalı güvenilir bir veri akışı sağlanırken, UDP protokolunda gönderilen veri paketlerinin hedef bilgisayara ulaşacağı garanti edilemez. Akış kontrolu sağlanmaz. UDP genellikle, gönderilen paketlerin sadece belirli bir aktif cihazı hedef aldığı uygulamalarda kullanılır.

TCP Protokolu

- TCP protokolu; bilgisayarlarda çalışan uygulamalar arasında;

  <İstemci IP adresi, Port No>, <Sunucu IP adresi, Port no> ikililerini temel alan bağlantı kurar. Her TCP bağlantısı bu ikililerle ifade edilir.
- IP protokolu bağlantısızdır. Dolayısıyla gönderilen paketlerin yerlerine ulaştığını garanti etmez. Bu açığı kapatmak için, bağlantılı ve güvenli veri akışını sağlayan TCP protokoluna ihtiyaç duyulur.
- TCP protokolunu kullanan uygulamalar veri göndermeden önce bağlantı kurmak zorundadaırlar.
- TCP , bağlantıda olan bilgisayarlar arasındaki güvenli veri iletişimini sağlayan, sanal devre mantığıyla çalışan bir protokoldur.
- **Hata denetimi yapar**
- **Güvenli veri iletimi sağlar.**
- **Bağlantıda olan bilgisayarlar arasında akış, tıkanıklık kontrolu sağlar.**
- **Çoklama (Multiplexing) yöntemiyle birden fazla bağlantıya izin verir.**
- **Sadece bağlantı kurulduktan sonra veri iletimi sağlar.**
- **Gönderilen mesaj parçaları için, önceli, güvenlik tanımlamaları yapılabilir.**

- TCP gönderdiği her parçayı numaralandırır. Bu no'lar kullanılarak, verilerin gönderildiği sıra ile alıcı tarafından alınması sağlanır.
- Gönderilen her veriye atanan dizi numarası sayesinde hangi verinin hedefe ulaşıp ulaşmadığı kontrol edilir. Dizi no TCP başlığı kısmındadır.
- Alıcı ise TCP bağlantısı ile aldığı her pakete karşılık yeni bir mesaj parçasını göndericiye bildirir. Bu mesajın başlığındaki ACK no'su ise gönderilmesi beklenen bir sonraki parçanın sıra numarasını da barındırır.
- TCP protokolu her iki yönde de veri akışına imkan sağlar (yani her iki trafta biribirlerine veri gönderebilirler. Gönderilen veriler byte (8 bitlik) gurupları şeklinde değerlendirilir.

- Bağlantı kurulması < [IP adres1, port no 1], [IP adres2, portno2]> gibi iki uç nokta arasında gerçekleşir. Seçilen port no'lar uçlardaki uygulamalar tarafından farklı şekilde seçilmiş olabilir. Biribirleriyle aynı olma zorunluğu yoktur.

- Yukarıdaki parametreler sayesinde bilgisayarlar arasında birden fazla TCP bağlantısı sağlanabilir.

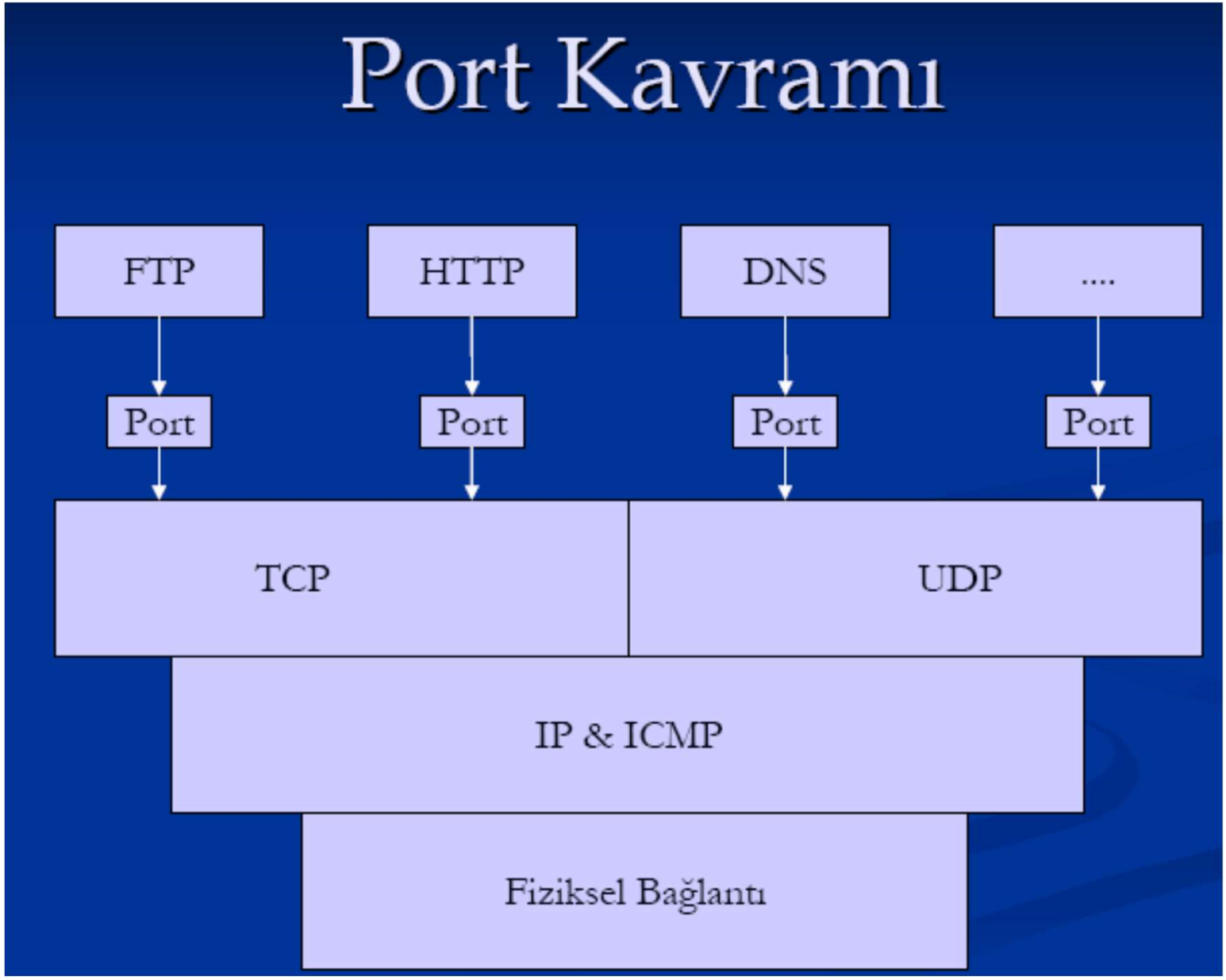
PORT KAVRAMI

- Bir Hos'tun diğer host üzerindeki değişik servisleri (hizmetleri) kullanabilmesi için veya değişik bilgisayarların aynı bilgisayardaki bir servisi kullanabilmesi için bu servisi tanımlayan adreslemeler vardır.

- TCP protokolunda her uçta 2^{16} tane farklı TSAP adresi tanımlıdır. Bu adreslere PORT denir.

- Uç düğümün 32 bitlik IP adresi ve 16 bitlik port adresinin beraber kullanılmasına soket no denir. Bir soketin blok şeması aşağıda verilmektedir.

Port Kavramı

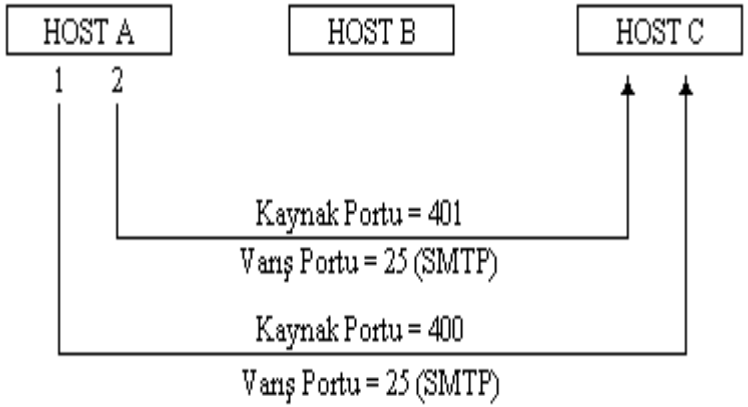


Transport (Ulaşım)Katmanı

Numara	İsim	Tanım
5	RJE	Uzaktan iş yürütme
7	ECHO	Eko
11	USERS	Aktif kullanıcılar
13	DAYTIME	Gündüz
20	FTP-DATA	Dosya transferi (veri)
21	FTP	Dosya transferi (kontrol)
23	TELNET	TELNET
25	SMTP	Basit mail transferi
37	TIME	Zaman
42	NAMESERV	Host isim sunucusu
43	NICKNAME	Takma-ad
53	DOMAIN	Domain name server
67	BOOTPS	Bootstrap protokol sunucusu
68	BOOTPC	Bootstrap protokol istekçisi
69	TFTP	Önemsiz dosya transferi
79	FINGER	Finger
101	HOSTNAME	NIC host ismi sunucusu
102	ISO-TSAP	ISO TSAP
103	X400	X.400
104	X400SND	X.400 SND
105	CSNET-NS	CSNET posta-kutusu isim sunucusu
109	POP2	Posta ofisi protokolü 2
111	RPC	SUN RPC portmap
137	NETBIOS-NS	NETBIOS isim servisi
138	NETBIOS-DG	NETBIOS datagram servisi
139	NETBIOS-SS	NETBIOS oturum servisi

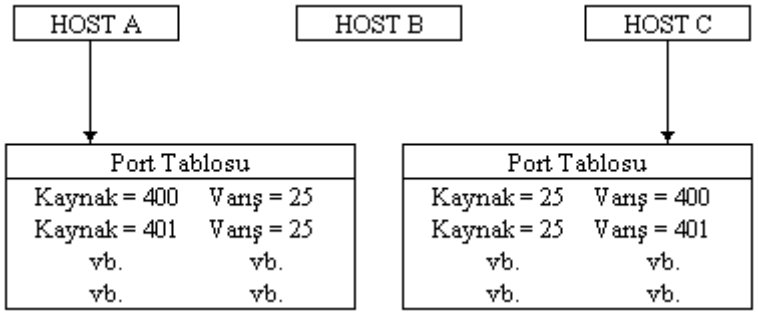
Port atama (Multiplexing-Çoklama)

- Aşağıdaki şekil'de, Birinci olayda, A host`u, C host`una bir TCP segmenti gönderir. Bu segment bir yüksek-seviye prosesi ile haberleşmek için bir TCP bağlantısı isteğidir. Burada SMTP`ye atanmış port 25 istenmektedir. Varış port değeri 25 olarak sabitlenmiştir. Ancak, kaynak port tanımlayıcısı bölgesel bir sorundur. Bir host cihazı iç işlemleri için herhangi bir uygun numara seçebilir.
- İkinci bağlantı ise, (şekilde 2 rakamı ile gösterildi) SMTP`yi kullanmak üzere C host`una yapılmıştır. Neticede, varış portu 25 aynıdır. Kaynak port tanımlayıcısı farklıdır; bu durumda 401`e set edilmiştir. SMTP erişimi için iki farklı numaranın kullanılması A host`u ve C host`undaki iki oturum arasında bir karışıklık olmasını engeller.



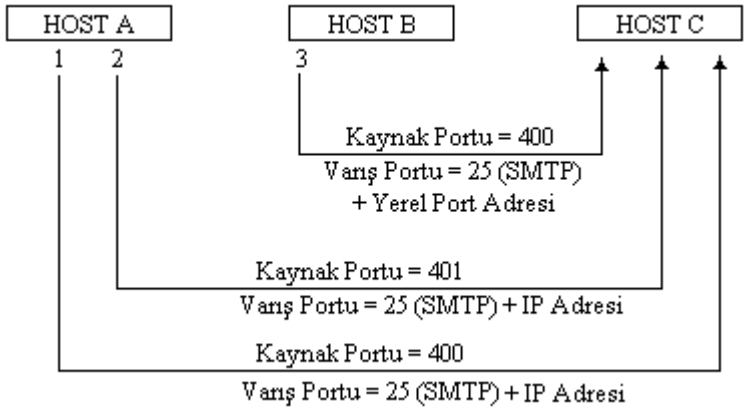
Port atama-2

- Şekil de, bir önceki iki segmentin nasıl bağlantı kurduğu gösterilmektedir. A ve C host`ları tipik olarak TCP bağlantıları ile ilgili bilgileri port tablolarında saklarlar.
- Dikkat edilirse bu tabloların kaynak ve varış değerleri arasında ters bir ilişki vardır. A host`unun port tablosunda, kaynaklar 400 ve 401, ve iki varış da 25`dir. C host`unda ise iki kaynak da 25, ve varışlar 400 ve 401`dir. Bu suretle, TCP modülleri ileri ve geri haberleşebilmek için kaynak ve varış port numaralarını terslerler.



Port atama -3

- Başka bir host`un C host`una aynı kaynak ve varış port değerleri ile bir bağlantı isteği göndermesi olasıdır. Varış port değerlerinin aynı olması olağandışı değildir. çünkü iyi-bilinen portlara sıklıkla ulaşım isteği vardır. Bu durumda, varış portu 25 SMTP`yi tanımlayacaktır. Kaynak port tanımlayıcıları bölgesel bir olay olduğundan Şekil'de gördüğümüz gibi B host`uda kaynak portunu 400 olarak seçmiştir.
- Ek bir tanımlayıcı olmaksızın, A ve C host`ları arasındaki ve B ve C host`ları arasındaki bağlantılarda çakışma olacaktır çünkü her iki bağlantı da aynı varış ve kaynak port numaralarını kullanmaktadır. Bu gibi durumlarda, C host`u datagramların IP başlıklarındaki IP adreslerini kullanarak ayrımı kolayca başarır. Bu durumda kaynak portları ikilenir ancak internet adresleri oturumları farklılaştırır.



TCP Protokolu Mesaj Yapısı

Kaynak ve hedef portlar, servis noktalarının sağlanması içindir. İlk 1023 port no'su IANA tarafında kullanılan standart port nolarıdır.Uygulamalar diğer port nolarını diledikleri gibi seçerler.

Sıra (dizi) no ve onay (Ack-Bilgi) no kısımları bağlantı güvenliği için kullanılan parça sıra no ve alıcı tarafından beklendiği bildirilen (alıcı tarafında) parça no kısımlarıdır.

Bayrak alanı

ACK =1 bilgi numarasının geçerli olduğunu belirtir.

SYN =1 Bu durum TCP bağlantısının kurulacağını belirtir.

FIN =1 Bağlantının sonlanacağını bildirir.

RST = 1 bağlantının fazla hatalı olduğu, sonlandırılacağı anlamındadır.

PSH =1 TCP modülü aldığı veriyi acilen üst katmana gönderir.

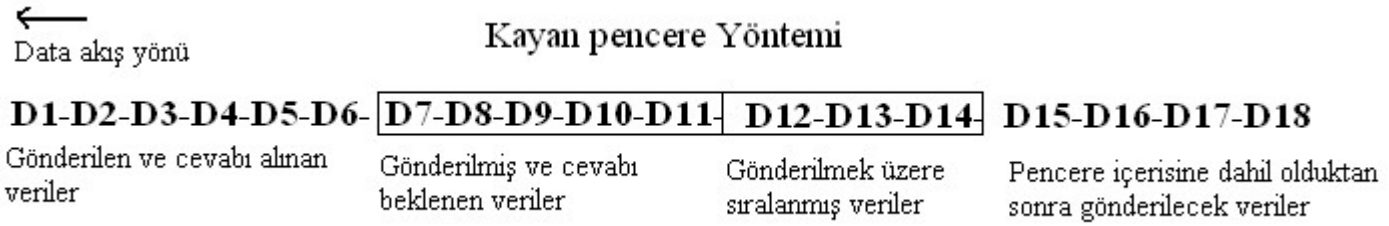
URG =1 alıcıya, aldığı dataları işlemeden band dışı veri gönderilmesine izin verir.

TCP bağlantıları,"üç adımda uzlaşma" **Three Way handshaking** yöntemiyle kurulur.

SYN=1 ve ACK=0 bağlantı açma isteği
SYN=1 ve SYN=1 bağlantı açma onayı
SYN=0 ve ACK=1 Veri Paketi veya ACK paketi

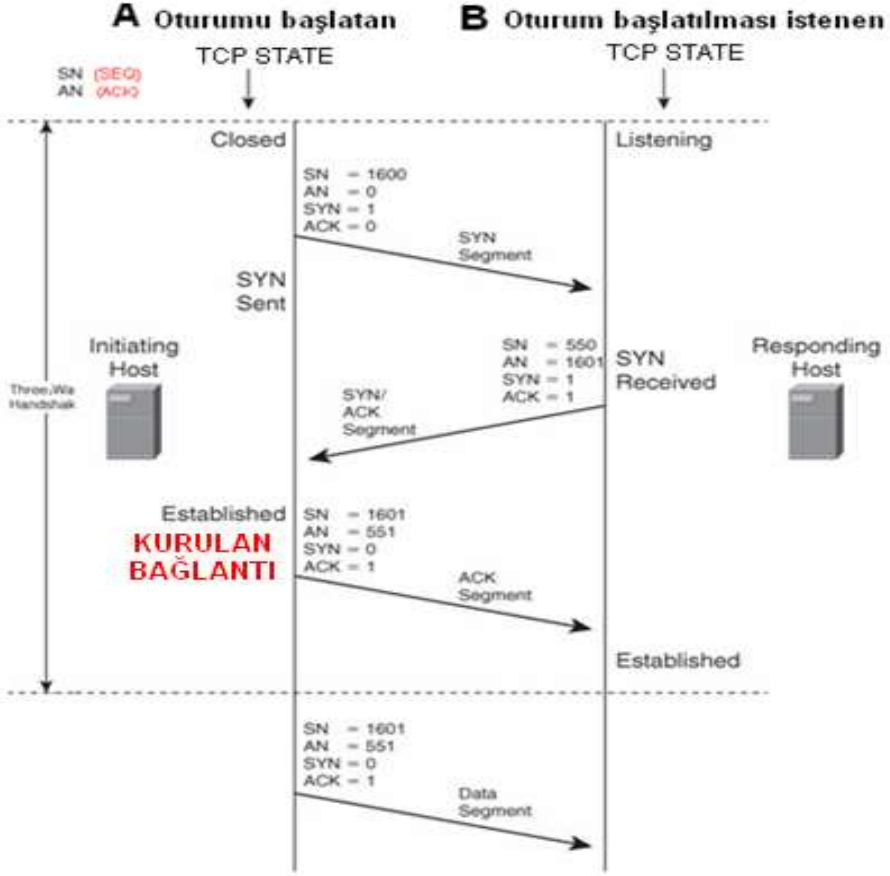
Pencere (Window) Alanı:

- Bu alan alıcı tarafından kullanılır ve ***veri akışını kontrol*** eder. Bu alan gönderilmesi gereken oktet miktarını belirler. Pencere alanı kullanılarak alınan paketler için tekbir bilgi paketi gönderilmesi sağlanır. Bu durum veri akışını hızlandırır.
- Alıcı gelen verileri aldıktan sonra, karşı tarafa bilgi paketi ile beraber, kabul edebileceği büyüklükteki dizi numarasının da gönderir. Kabul edilebilir dizi numarası aralığına pencere denir. Pencere, alıcı tarafının onayı ile , göndericinin iletebileceği oktet sayısını belirler.
- Böylece, gönderici verilerin alındığına dair bilgi messajı almadan belirtilen miktarda veri transferi yapabilir. Buda protokolun veri iletim hızını arttırır.



TCP protokolunda bağlantı açma (Three way handshake)

TCP bağlantı başlatma yordamı iletişim noktaları arasında üç paket iletim gerektirdiğinden genellikle üç-yollu el sıkışma denir. Başlatan bilgisayar **(A)**, yeni bağlantı için bir rastgele başlangıç sıra numarası (ISN –İnital service-sıra no) seçer ve daha sonra SYN biti=1 ve ACK biti =0 olarak ayarlanmış ilk paket gönderir. Bu pakete SYN denir



SYN alan **B** (yanıt veren), yeni bir bağlantı için bir ISN (Başlangıç dizi no- örn.550) seçer ve sonra **SYN biti=1 ve ACK biti =1** olacak şekilde cevap gönderir. Bu paket SYN / ACK Onay paketidir. ACK no alanına ise A (oturumu başlatan)'ın SYN paketindeki SEQ' no +1 yapar.

A bu SYN / ACK onay paketini aldıktan sonra; oturumun kabul edildiğini anlar. SYN bit=0 ve ACK biti= 1 yaparak, yeni segmenti B'ye gönderir. AN no'sunu 1 arttırır (551- Alıcının gönderdiği paketteki ISN No'sunu). Sıra Numarası (SN) alanına veri olmamasına rağmen, A'nın paketindeki ISN'yi bir arttırır. Bu ACK segmentinin tek amacı A ve B 'nin bu işle ilgili sayaçlarının senkronizasyonudur. Daha sonraki paketler veri taşır.

Bağlantının koparılması

- **Gönderilen herbir veri parçasının (segmentin) ağ üzerinde kalabileceği bir belirli yaşam süresi vardır. Buna MSL (maximum Segment Life) denir.**
- **TCP segmentleri alıcısına iletildiği zaman , datagramları gönderen bilgisayar pencere alanını ilerletebilmek için , karşı tarafın bilgi paketi (ACK) göndermesini bekler. Bu bekleme süresine "zaman aşımı" (time –out interval)denir.**
- TCP bağlantısnın sonlandırılması isteği için FIN bayrağı =1 olan bir segmentler oluşturulup gönderilir.
- Bağlantının koparılması için her ,ki uç noktanın da FIN bayrağını kullanması gerekir.
- Her iki ucun birlikte karar vererk bağlantının kesilmmesi işlemine; zarif kapanış (graceful close) denir.
- Eğer taraflardan birisi diğerine haber vermeden bağlantıyı sonlandırırsa veri kaybı olabilir.

Kısa özet

Hizmet veren bir TCP portu açıksa kendisine gelen SYN paketine karşılık olarak ACK+SYN paketi döner. Dönen paketlerden ACK (onay paketi), SYN ise hizmet veren tarafın istek başlatma paketidir.

Port kapalıysa RST döner, SYNflood saldırısının başarılı olabilmesi için portun açık ve dinlemede (LISTEN mod) olması gerekir.

UDP (User Datagram Protocol)

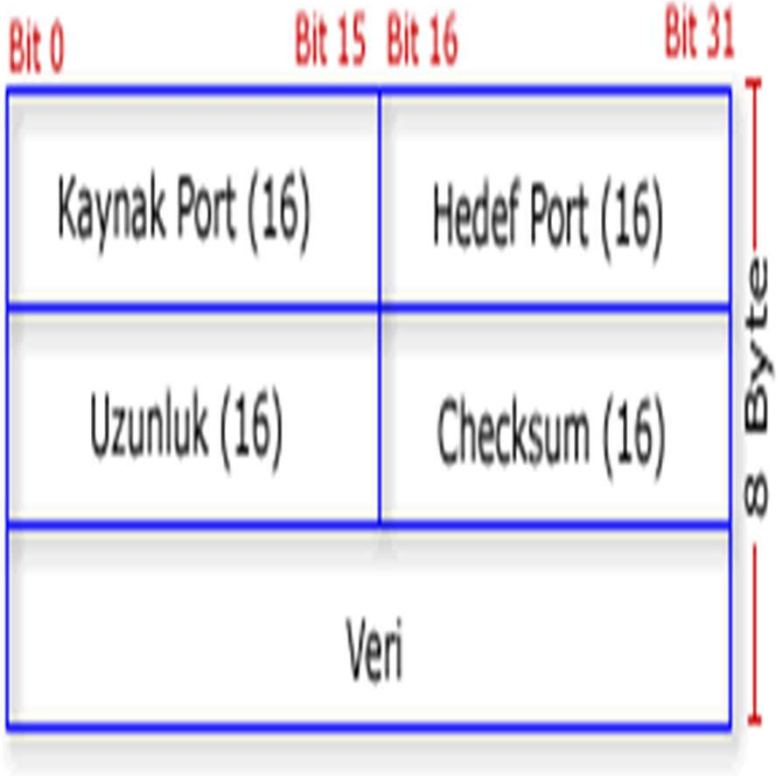
Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir prosedür içerir.

UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

- Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır.
- UDP bağlantı kurulum işlemlerini,akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir.
- UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

UDP paket formatı

- **kaynak port**: Opsiyonel bir alandır. Gönderilen işlemin portunu gösterir. Eğer gönderen host bir kaynak numarasına sahip değilse bu alan “0” ile doludur
- **hedef port:** Hedef host içerisinde, işlemlere uygun ayrımları yapmak için kullanılır. Hedef port internet adresleri parçalarının genel durumunu içerir.
- **Uzunluk:** UDP veri ve UDP başlığının bayt cinsinden toplam uzunluğudur.minimum 8 bayttır
- **Checksum:** IP ve UDP başlığı ve verinin bilgisini içeren yalancı başlıgın toplamı olan birbirinin tamamlayıcısı 16 bitten oluşur. Opsiyonel bir alandır. Hata kontrol mekanizması sağlar. Eğer hata kontrolü yapılmayacaksa bu alan “0” ile doludur.
- **Veri:**Opsiyonel



UDP ile TCP 'nin farkları

Servis	TCP	UDP
Bağlantı kurulumu	Zaman alır ancak TCP bunu güvenli şekilde yapar.	Bağlantıya gerek yoktur.
Teslim garantisi	Gönderildiğini onaylar.	UDP onay mesajı göndermeden,alıcı paketin alındığına dair sinyal göndermez.Kaybolan paketler tekrar iletilmez.
Paket ardışıklığı (paketlerin doğru sırası hakkında bilgi)	Ardışık numaralanmış paketler	UDP ardışıklık numarası vermez. Paketlerin sürekli ulaştığı veya kaybolduğu düşünülür.
Akış kontrolü	Alıcı göndericiye yavaşlaması için sinyal gönderebilir.	Paket akış kontrolü için TCP' de kullanılan onay UDP' de geri dönmez.
Tıkanıklık kontrolü	Network cihazları TCP onayları sayesinde göndericilerin tavrını kontrol edebilir.	Onay olmadan network tıkanıklık sinyali gönderemez.

TCP protokoluna yönelik saldırılar

- TCP protokolunun tasarım özelliklerinden dolayı iki önemli zayıf noktası vardır.

  - Protokol, TCP bağlantısı kurma isteği **“SYN Bombardımanı-SYN Flooding”** karşısında zayıf kalır : SYN flooding genellikle serverlara yapılan bir saldırı türüdür. Amacı çok sayıda

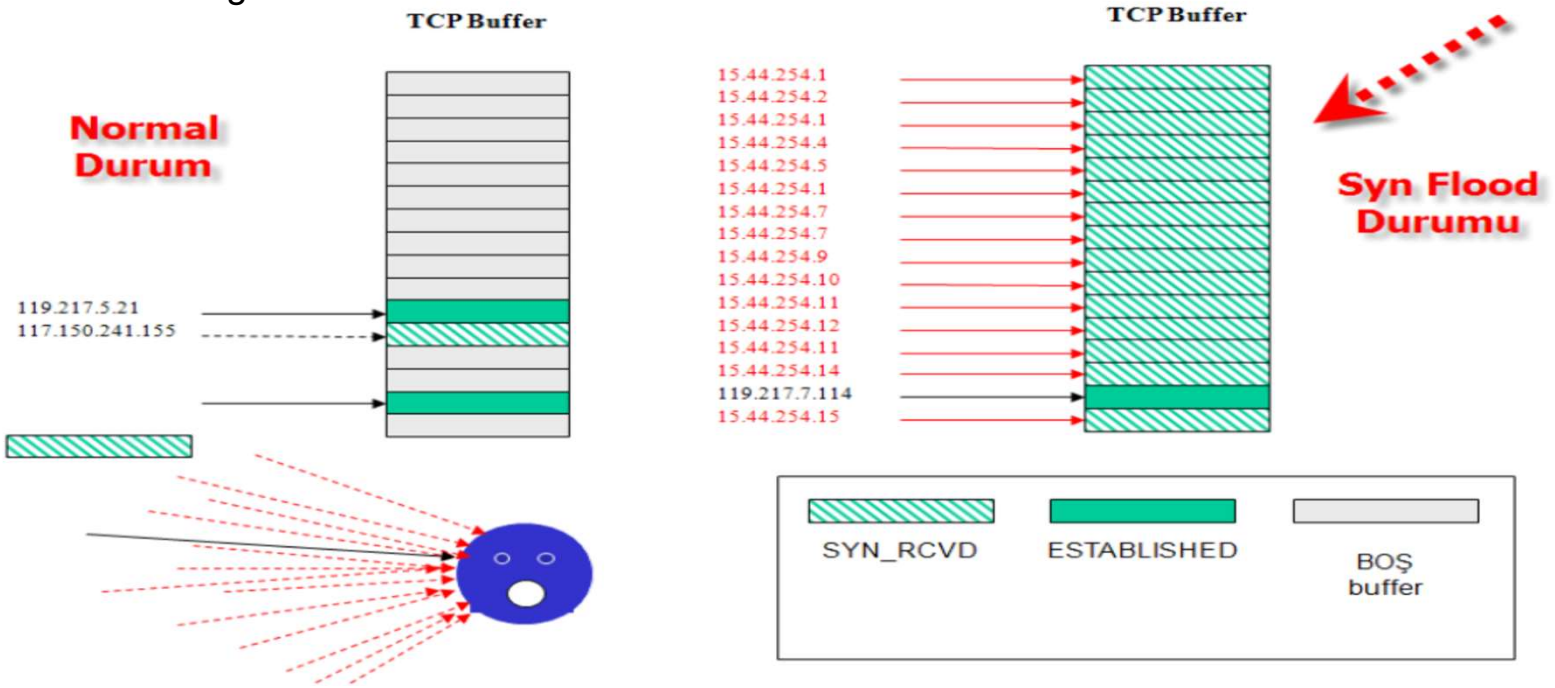
  “ Bağlantı istek Paketi” hazırlayıp sunucuya göndererek hizmetleri aksatmaktır .

  - Protokol **“TCP oturumu ele geçirme “** saldırıları karşısında zayıf kalır. “TCP oturumunu ele geçirme”; iki bilgisayar arasında üç adımda sağlanan TCP bağlantısının birtakım yöntemlerle ele geçirilmesi veya veri akışına ; bağlantı içerisinde yer almaması gereken verileri eklemektir.

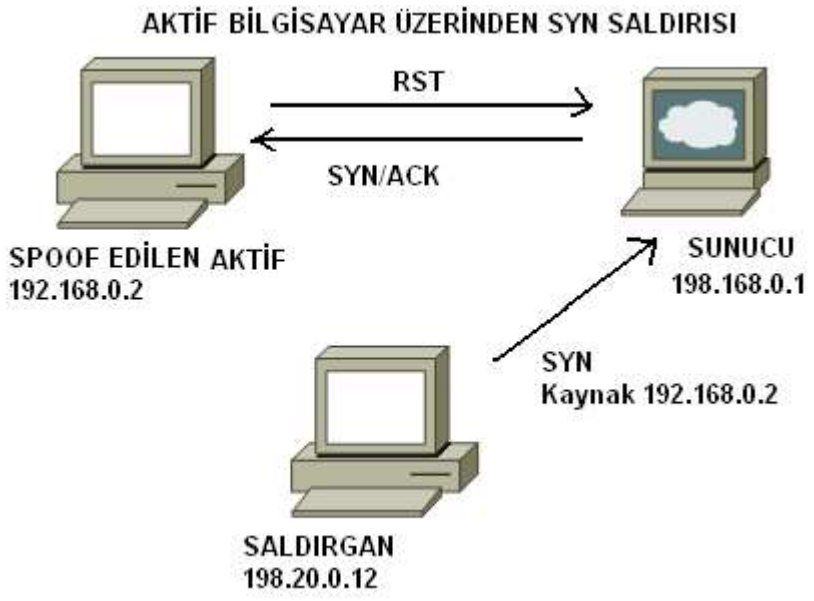
SYN FLOOD atakları

- SYN Flooding (SYN Bombardımanı) sunucunun başedemiyeceği kadar fazla “bağlantı kurma isteği” paketlerinin ağ üzerine bırakılması ile gerçekleştirilir.
- Saldırganlar, sunucuya sadece **1. syn paketini** gondererek gelen **2. pakete** karsilik **3. syn onay mesajini** gondermeden araliksiz olarak **1. syn paketi (oturum acma istegi**) gonderebilir.
- Sunucunun kapasitesinde acilabilecek oturum sayisi rakamlarla ifade edilmis ise kisa sure icerisinde bu syn paketleri ile oturum acma istekleri tamamen rezerve hale getirilir.
- Sunucu 3. syn paketini almadiğı sürece belirtilen zaman kadar bekleyerek oturum islemini rezerve eder ve belirtilen sure dolmadan bu oturum isteğini kapatamaz.
- Yuzlerce hatta binlerce oturum acma istegi karsisinda sunucu kısa süre sonra yanit veremez hale gelir ve artik islevini yerine getiremez.
- Bu saldırı türü, sunucunun mümkün olduğu kadar pasif çalışmasını hatta bağlantı isteklerine hiçbir şekilde cevap verermemesini amaçlar.
- Bu bir DOS saldırısıdır.

Syn Flood saldırısı, açık bir porta (dinlemede olan port), sistemin kapasitesinden **(Backlog Queue)** fazla gönderilecek SYN paketleriyle gerçekleştirilir. İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan **TCB (Transmission Control Block)** olarak adlandırılır . Bu alanların toplamı **Backlog queue (Birikim kuyruğu)** olarak adlandırılır. Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini backlog queue veriyapısı belirler. Bu değer her işletim sisteminde vardır ve ön tanımlı olarak düşük bir değerdir (256 gibi).
Synflood saldırılarında tüm mesele backlog queue'nin dolması ve yeni gelen bağlantıların reddedilmesidir. Backlog queue değerinin büyük olması demek daha fazla half-open(SYN paketi) bağlantı kabul edebilmek demektir. SYNFlood saldırılarında backlog değeri arttırılarak saldırıya karşı ek önlem alınabilir.Backlog queue dolmasıyla birlikte işletim sistemi yeni bağlantı kabul edemez ve bu esnada sunucuya bağlanmaya çalışanlar bağlanamazlar ki bu da SYN Flood saldırısına denk gelir.



- SYN flood saldırısı için spoof edilmiş (taklit edilmiş) IP datagramlar kullanılır. Yani bağlantı kurma istek segmentini taşıyan paketlerin gönderici IP'sine spoof edilmiş veya yapay olarak yaratılmış adresler atanır.
- Taklit edilmiş paketler ile pasif bigisayar saldırısı için, seçilen IP adresine, IP datagramların yönlendirilebilir olması fakat , bilgisayarın erişilebilir olmaması gerekir (Sunucu onay segmentini gönderip oturumun senkronizasyonunu sağlayan üçüncü paketi bekleyecektir.)
- Taklit edilmiş paketler için aktif bigisayar saldırılarında; Sunucunun gönderdiği SYN/ACK paketlerine, aktif bigisayar, RST =1 olan datagramlar gönderir. Bu paketi alan sunucu bağlantı isteğini sonlandırır. Hafızadaki yerini temizler.



Synflood Önleme Yöntem ve Çeşitleri

SynFlood saldırılarına karşı çeşitli önlemler geliştirilmiştir. Bunlar arasında önemlileri;

- Syncookie
- Syncache (FreeBSD default)
- SynProxy
- TCP Authentication

SynCookie

Normal TCP bağlantılarında gelen SYN bayraklı pakete karşılık ACK paketi ve SYN paketi gönderilir. Gönderilen ikinci (sunucunun gönderdiği) SYN paketinde ISN (Sıra no) değeri random olarak atanır ve son gelecek ACK paketindeki sıra numarasının bizim gönderdiğimizden bir fazla olması beklenir, son paket gelene kadar da sistemden bu bağlantı için bir kaynak ayrılır (backlog queue).Eğer bizim gönderdiğimiz SYN paketine dönen ACK cevabı bizim ISN+1değilse paket kabul edilmez.

Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz, bunun aksine SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanır (kaynak.ip + kaynak.port + hedef.ip + hedef.port + x değeri) ve hedefe gönderilir, hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur, değilse bağlantı kurulmaz.

Böylece spoof edilmiş binlerce ip adresinden gelen SYN paketleri için

sistemde bellek tüketilmemiş olacaktır ki bu da sistemin SYNflood saldırıları

esnasında daha dayanıklı olmasını sağlar.

Syncookie mekanizması **backlog queue** kullanmadığı için sistem kaynaklarını daha az tüketir. Syncookie aktif iken hazırlanan özel ISN numarası cookie olarak adlandırılır.

İstemci tarafı syncookie özelliği İnverse syn cookie (Scanrand aracı) araçları kullanılarak syncookie engellemesi aşılabilir. Bu durumda da bir ip adresinden gelecek max bağlantı sayısı limitlenerek saldırı engellenmiş olur.

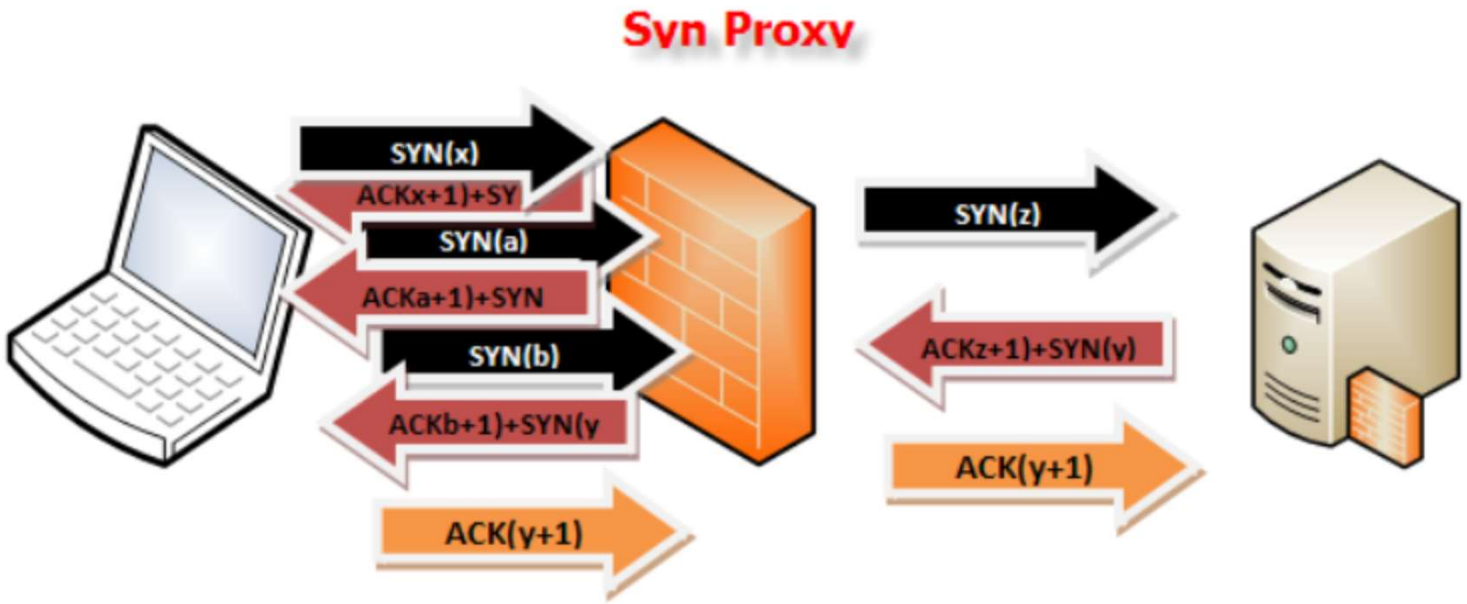
Syncookie'de özel hazırlanacak ISN'ler için üretilen random değerler sistemde matematiksel işlem gücü gerektirdiği için CPU harcar ve eğer saldırının boyutu yüksekse CPU performans problemlerinden dolayı sistem yine darboğaz yaşar. DDOS Engelleme ürünleri(bazı IPS'ler de) bu darboğazı aşmak için sistemde Syncookie özelliğini farklı özel bir CPU'ya devredeler.

SynCache nasıl çalışır?

LISTEN modundanki bir portun gelen SYN paketlerinde bellekten bir alan ayırdığını ve bu alanın belirli boyutlarda olduğundan bahsetmiştik. SynCache özelliği , gelen SYN paketleri için TCB değerinden daha az yer kaplayan başka bir veri yapısı kullanmayı önerir. Böylece sisteme gelen SYN paketlerinde daha az bellek alanı harcanır(Normalde 700 Byte civarı, 160 Byte Syncache kullanıldığında). Fakat yoğun bir saldırı da bu özellik kısa sürede işe yaramaz hale gelecektir. Bu sebepledir ki Syncache tek başına synflood saldırılarına karşı efektif bir koruma sağlamaz. Syncookie'i tetikleyici olarak kullanılır. Yani sistemde öntanımlı olarak syncookie aktif edilmez, syncache aktif edilir. Syncache belli bir değerin üzerinde SYN paketi almaya başladığında SYNCookie'ei tetikler vesistem koruma moduna geçer.

SynProxy

SynProxy, SYN paketlerine karşı proxylik yapmaya yarayan bir özelliktir. Güvenlik duvarlarında ve Syncookie'nin kullanımının sıkıntılı olduğu durumlarda rahatlıkla kullanılabilir. Syncookie gibi arkasında korumaya aldığı sistemlere gelecek tüm SYN paketlerini karşılar ve üçlü el sıkışma tamamlandıktan sonra paketleri koruduğu sistemlere yönlendirir



TCP Oturumunu ele geçirme saldırıları

- Sunucu –istemci arasında açılmış olan bir oturumu ele geçirmek için birkaç adımlı işlem yapmak gerekir.

- **Sunucu-İstemci arasındaki var olan TCP bağlantısının belirlenmesi:** Hangi kullanıcıların ne kadar süreyle nerelerle bağlantı kurduklarının bilinmesi için bilgi toplama çalışması yapılmalıdır. Sunucu/İstemci arasındaki bağlantı tespiti için; "NBTSTAT, Fingerprint, ve uzak sistemler için rpcinfo bu komutlardan bazılarıdır. komutlardır.
- **Sunucunun bağlantı sırasında datagramları için atadığı dizi numarasının tepit edilmeye çalışılması :** TCP protokolu diğer bilgisayarlardan gelen doğru dizi numarasına sahip bütün paketleri "güvenilir" ve bağlantısı yapılmış bilgisayardan geliyor kabul eder. ISN no'sunun tahmin edilebilir olması, bağlantı içerisinde yer alan bilgisayarlara ait taklit edilen paketlerin oluşturulmasına sebep olabilir. Bazı işletim sistemlerinde ISN kodlarını yaratan algoritmalar bilindiğinden bu no'ların tespit edilmesi kolaylaşabilir.
- **"SYN Flooding" ile sunucunun susturulması ve oturumun ele geçirilmesi.**

UDP Portlarından Saldırılar

- UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir, gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

UDP Portlarından Saldırılar

- Bir bilgisayar üzerinde veya birkaç bilgisayar arasında,UDP portlarına yöneltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise, ağ 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 Portlarından Saldırılar

- Örneğin 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, rastgele 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.

EK BİLGİ

Echo servisi kendisine gönderilen her şeyi tekrarlar ve **chargen** hizmeti sürekli bir veri akışı oluşturur. Birlikte kullanılırsa, sonsuz bir döngü oluşturur ve hizmet reddine neden olur.

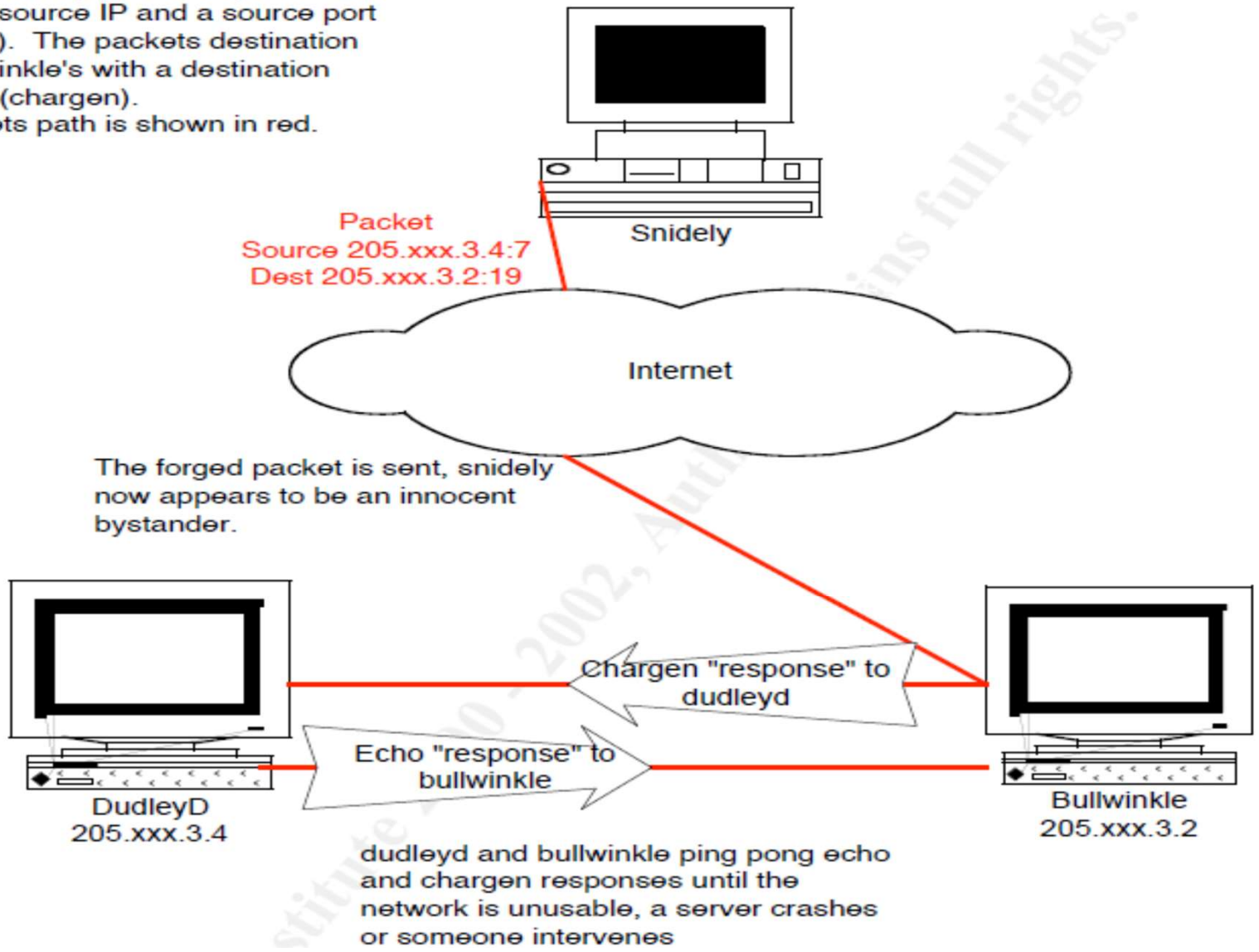
Bir ana bilgisayarda chargen hizmeti çalışıyor ise; **Chargen s**ervisi, test ve ölçüm amaçlıdır ve hem TCP hem de UDP protokollerini dinleyebilir.

TCP bağlantısı açıldıktan sonra, sunucu bağlanan ana makineye rastgele karakter göndermeye başlar ve ana bilgisayarlar bağlantıyı kapatana kadar devam eder.
Protokolün UDP sürümünde, sunucu, bağlanan ana bilgisayardan bir UDP paketi aldığında rastgele bir sayı (0 ila 512 arasında) içeren bir UDP paketi gönderir. Sunucu tarafından alınan herhangi bir veri atılır.

Chargen hizmeti, bir bilgisayardaki bir hizmetten başka bir bilgisayardaki başka bir hizmete veri göndermek için taklit edilebilir. Bu eylem sonsuz bir döngüye neden olur ve bir hizmet reddini saldırısı yaratır.

Diagram of a UDP Flood

The NPC snidely creates a packet with dudleyd's source IP and a source port of 7 (echo). The packets destination IP is bullwinkle's with a destination port of 19 (chargen).
The packets path is shown in red.



UDP Portlarından Saldırılar

- Böyle bir saldırı sonucunda doğabilecek sonuçlar şunlardır:
  - Saldırının yöneltildiği servisler kilitlenebilir.
  - Bu servisleri veren bilgisayarların performansı düşebilir
  - Servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırır.
- Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servisleri bilgisayarın üzerinden kaldırmak gelir.

UDP Portlarından Saldırılar

- Bu yaklaşımı kullanırken iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir.

- Bu saldırılarda en çok kullanılan UDP servisleri **chargen** ve **echo** servisleridir. Bu servisler neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.

- Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan programların kurulması faydalı olacaktır.

UDP Flood Saldırısı

- UDP Flood saldırısı host tabanlı servis dışı bırakma saldırılarından biridir.
- UDP Flood atağı saldırganın hedef sistemin rastgele bir portuna UDP paket göndermesiyle yapılır.
- Saldırgan, saldırının etkisini arttırmak için zombi bilgisayar denilen, saldırganın önceden üzerine casus yazılım yükleyerek ele geçirdiği sistemleri kullanır.
- Böylece hem kendi IP adresini saklamış olup yakalanma riskini azaltır hem de binlerce zombi bilgisayarı kullanarak atağın kuvvetini arttırır.

UDP Flood Saldırısı

- Hedef sistem bir UDP paket aldığında hedef portta hangi uygulamanın beklediği hesaplanır.
- Portta bekleyen uygulama olmadığı anlaşılınca erişilemeyen sahte IP adreslerine bir ICMP paketi üretilir ve her paket için 60 sn beklenir. Bu saldırı ağda tıkanıklık ya da kaynak doluluğuna sebep olur.
- UDP trafiğinin TCP trafiğine önceliği vardır. TCP protokolünün uzun sürede gelen paket onayları karşısında tıkanıklığı kontrol eden bir mekanizması vardır: bu mekanizma gönderme aralığını düzenleyerek tıkanıklık oranını azaltır.
- UDP protokolü bu mekanizmaya sahip değildir. Bir süre sonra tüm bant genişliğini kullanarak TCP trafiğine çok az yer bırakır.
- Eğer yeterli UDP paket hedef sistemdeki porta gönderilirse sistem çöker ve servis dışı bırakılır.