

## IRC/mIRC ile alakali dokumanlar > TCP/IP Nedir

### TCP/IP Nedir

Internetin belkemiği olan TCP/IP ile ilgili bazı temel bilgileri bilmeden ne dönüp bittigini anlamak zordur. Bu yüzden internet savaslari konusunda ayrıntiya girmeden &ouml;nce kısaca TCP/IP protokolüne deginmek istedim.

Bu konuda kısaca TCP/IP'nin ne oldugunu ve nasıl &cedil;alistigini g&ouml;recegiz. Burda verilen bilgiler temel d&uuml;zeydedir ve ileride g&ouml;recegimiz konulari daha kolay anlamaniza yardimci olacaktır.

#### 1- Nedir TCP/IP

TCP/IP internette veri transferi i&cedil;in kullanılan iki protokolü temsil eder. Bunlar Transmission Control Protokol (TCP) ve Internet Protocol (IP). Ve bu protokoller de daha geniş olan TCP/IP protokol grubuna aittir. TCP/IP'de bulunan protokoller internette veri transferi i&cedil;in kullanilir ve internette kullanılan her t&uuml;r&uuml; servisi saglarlar. Bunlari arasında elektronik posta transferi, dosya transferi, haber gruplari, WWW erisimi gibi servisler TCP/IP sayesinde kullanıcılara sunulmaktadır.

TCP/IP protokol grubunu ağ seviyesi protokolleri ve uygulama seviyesi protokolleri olarak iki gruba ayirabiliriz.

Ağ seviyesindeki protokoller genellikle kullanıcıya g&ouml;r&uuml;nmeden sistemin alt seviyelerinde &cedil;alisirlar. &Ouml;rnek olarak IP protokol&uuml; kullanıcıyla uzak bir makine arasındaki paket iletimini saglar. IP ağ seviyesinde diğeri protokollerle etkilesimli olarak &cedil;alilarak paketlerin hedef adrese g&ouml;nderilmesini saglar. &Ccedil;esitli ağ ara&cedil;lari kullanmadiginiz s&uuml;rece sistemdeki IP trafiginin ve neler d&ouml;n&uuml;p bittigini anlayamazsiniz. Bu ara&cedil;lar ağda gidip gelen IP paketlerini yakalayabilen sniffer'laridir. Sniffer'lar konusuna ileriki konularda ayrıntıyla degineceğiz.

Uygulama seviyesi protokolleri sistemde daha &uuml;st d&uuml;zeyde &cedil;alisirlar ve kullanıcıya g&ouml;r&uuml;n&uuml;rler. &Ouml;rnek olarak Dosya Transfer Protokol&uuml;n&uuml; (FTP) verebiliriz. Kullanici istedigini bir bilgisayara bağlantı isteginde bulunur ve bağlantı yapıldiktan sonra dosya transferi islemini ger&cedil;eklestirir. Ve bu karşılıklı transfer islemleri kullanıcıya belli bir seviyede g&ouml;r&uuml;n&uuml;r, giden gelen byte sayısı, meydana gelen hata mesajlari... gibi.

Kısaca TCP/IP internette veri transferini saglayan protokoller grubudur.

Burda TCP/IP'nin tarih&cedil;esine girmeyeceğim s&ouml;yleyeceğim tek şey TCP/IP diğeri protokollere g&ouml;re &cedil;ok fazla avantaja sahip oldugu i&cedil;in &cedil;ok kısa s&uuml;rede en yaygın kullanılan protokol haline gelmiştir. Artık internetin belkemiği haline gelen TCP/IP herhalde &uuml;zerinde en &cedil;ok &cedil;alisilan ağ protokol&uuml;d&uuml;r.

G&uuml;n&uuml;m&uuml;zde artık TCP/IP sadece internet değil bir &cedil;ok alanda kullaniliyor. Intranet'ler mesela TCP/IP kullanılarak olusturulmaktadır. Bu tip bir sistemde TCP/IP'yi kullanmak diğeri protokollere g&ouml;re avantajlar i&cedil;erir. En basitinden TCP/IP hemen hemen her t&uuml;r&uuml; sistemde desteklendigi i&cedil;in &cedil;ok kolay bir şekilde heterojen sistemler kurulabilir. İşte internette tamamen heterojen bir sistem oldugu i&cedil;in TCP/IP en uygun protokold&uuml;r.

TCP/IP protokol&uuml; g&uuml;n&uuml;m&uuml;zde artık hemen hemen t&uuml;m işletim sistemlerinde desteklenmektedir. UNIX, DOS (Piper/IP ile), Windows (TCP/IP ile), Windows 95/98/2000/Me, Windows NT, Machintosh (MacTCP), OS/2, AS/400 OS/400 sistemlerinde TCP/IP desteği gelmektedir. Tabi her sistemin TCP/IP ger&cedil;eklemesi farklı olduğundan servis kalitesi de farklılıklar g&ouml;sterebilir. Ancak temel olarak sunulan servisler aynıdır ve

birbiriyle uyumlu olarak &cedil;alisirlar.

### 3.2- TCP/IP'nin Isleyisi

TCP/IP protokol yiginini kullanarak &cedil;alisir. (TCP/IP Stack) Bu yigin iki makine arasindaki veri transferini saglamak i&cedil;in gereken t&uuml;m protokollerin birlesmis bir halidir. Bu yigin kisaca en &uuml;stte 'uygulama seviyesi', daha sonra 'transport seviyesi', 'ag seviyesi', 'datalink seviyesi' ve 'fiziksel seviye'\lerden meydana gelir. Bu seviyelerde en &uuml;stte yakin olan seviyeler kullaniciya daha yakindir, alta yakin olan seviyeler ise kullanicidan habersiz olarak &cedil;alisan seviyelerdir. &Ouml;rnek olarak en &uuml;st d&uuml;zey olan uygulama seviyesinde FTP, Telnet gibi programlari &ouml;rnek verebiliriz. Bu programlari &cedil;alistirdiginizde diger sisteme bir baglanti kurulur ve veri transferi yapilir. Siz sadece yaptiginiz islemlerle ilgili sonu&cedil;lari ve olaylari g&ouml;r&uuml;rs&uuml;n&uuml;z ancak bir veri g&ouml;nderdiginizde bu veri ilk &ouml;nce sizin bilgisayarinizdeki bu TCP/IP protokol yigininde asagiya dogru inmek zorundadir. Yani uygulama seviyesinden, ftp'de verdiginiz bir komut mesela, transport seviyesine, ordan ag seviyesine ve en sonunda fiziksel seviyeye iner ve artik diger bilgisayara ulasmak &uuml;zere internet aginda yada yerel bir agda uzun yolculuguna baslar. Gidecegi makinenin fiziksel seviyesine ulasana kadar veriler genellikle bir yada daha fazla ag ge&cedil;idinden ge&cedil;erler. (tracert komutu belirli bir hedefe hangi ge&cedil;itlerden ge&cedil;erek gidilecegini veren komuttur) En sonunda diger makineye ulasinca yine uygulama seviyesine ulasincaya kadar, bu sefer karsida &cedil;alisan ftp sunucusuna, yine bu TCP/IP protokol seviyelerini bir bir yukari dogru asmak zorundadir.

Bu arada bu seviyelere ne gerek var diyebilirsiniz. Ancak bu seviyelerin her biri degisik bir g&ouml;revi &uuml;stlenmektedir. Bir seviye fiziksel olarak verilerin g&ouml;nderilmesi isini yaparken baska bir seviye verileri ufak paket dedigimiz par&cedil;aciklara b&ouml;lerek iletisim isini &uuml;stlenir, baska bir seviye ise iletisimde meydana gelebilecek hatalari tespit eder. Bu sekilde t&uuml;m seviyeler bir uyum i&cedil;inde &cedil;alisirsar ve her seviye karsi tarafta bulunan yine kendi seviyesindeki protokolle karsilikli iletisim i&cedil;indedir. Daha yukarida yada daha asagidaki bir seviyede ne gibi bir isin yapildigina ve sonu&cedil;lariyla ilgilenmez.

#### 3.2.1 Protokoller

Kisaca TCP/IP protokol yigininin nasil &cedil;alistigini g&ouml;rd&uuml;k ve simdi kullanılan protokollere bir g&ouml;z atalim.

##### Ag seviyesi protokolleri

Ag seviyesi protokolleri veri transferi islemini kullanicidan gizli olarak yaparlar ve bazi ag ara&cedil;lari kullanilmadan farkedilemezler. Bu ara&cedil;lar Sniffer'\lardir. Sniffer bir cihaz yada bir yazilim olabilir ve ag &uuml;zerindeki t&uuml;m veri iletisimini izlemeye yarar. Bu ara&cedil;larin kullanilis maksadi agda meydana gelebilecek hatalari tespit etmek ve &cedil;ouml;zmehtir. Ancak ileride de g&ouml;recegimiz gibi sniffer'\lar da hacker ve cracker'\lar tarafından kullanılan &ouml;l&uuml;mc&uuml;l makineler haline gelmistir.

Ag protokolleri arasinda &ouml;nemli olarak Adres &cedil;ouml;z&uuml;mleme Protokol&uuml; (ARP), Internet Mesaj Kontrol Protokol&uuml; (ICMP), Internet Protokol&uuml; (IP) ve Transfer Kontrol Protokol&uuml; (TCP) protokollerini verebiliriz. Kisaca bu protokollerin ne is yaptigina bir bakalim:

ARP protokol&uuml;: internet adreslerini fiziksel adrese d&ouml;n&uuml;st&uuml;rme i&cedil;in kullanilir. Bir paketin bir bilgisayardan &cedil;iktiginde nereye gidecegini IP numarasi degil gidecegi bilgisayarın fiziksel adresi belirler. Iste bu adreste paketin gidecegi ip numarasi kullanilarak elde edilir. Ve bu islemden sonra paket hedef ip adresine sahip

bilgisayara gitmek için gerekli yönlendirmelerle yolculuğuna başlar. Bilgisayara takili olan ethernet kartlarının bir ethernet adresi vardır. Ve bu adres IP adresinden farklıdır. Bir paket makineden çıktığı anda gideceği adres diğer bir makinenin ağ kartıdır ve bu ağ kartı ile IP numarası arasında bir bağ yoktur. Paket bu karta gidebilmesi için kartın fiziksel numarasını bilmek durumundadır.

ARP adresi; zümlemek istediği zaman tüm ağa bir ARP istek mesajı gönderir ve bu IP adresini öğren yada bu IP adresine giden yol üzerinde bulunan makine bu isteğe cevap verir ve kendi fiziksel adresini gönderir. ARP isteginde bulunan makine bu adresi alarak verileri artık bu makineye gönderir.

ARP protokolü nasıl çalıştığını ve daha ayrıntılı bilgi isteyenler RFC 826 dokümanına bakabilirler.

Internet mesaj kontrol protokolü: ICMP protokolü; iki yada daha fazla bilgisayar arasında veri transferi sırasında meydana gelebilecek hataları ve kontrol mesajlarını idare eder. Bu nedenle ICMP ağ problemlerini tespit etmek için çok önemli bir protokoldür. ICMP protokolü kullanılarak elde edebileceğimiz bazı sorunlar: bir bilgisayarın ayakta olup olmadığını kontrol etmek, ağ geçitlerinin tıkanık olup olmadığını kontrol etmek gibi...

ICMP protokolünde bilinen en yaygın ağ aracı ping'dir. ping programı karşıdaki bir bilgisayarın çalışır durumda olup olmadığını kontrol etmek için kullanılır. Çalışması mantığı çok basittir, karşı bilgisayara echo paketleri gönderir ve geri gelmesini bekler. Eğer paketler geri gelmezse ping hata mesajı verir ve karşı bilgisayarın ağa bağlı ve çalışır durumda olmadığı anlaşılır.

Internet protokolü: IP protokolü; TCP/IP protokolü yiginde ağ seviyesine aittir ve tüm TCP/IP protokolü takımının paket iletimi işlemini sağlar. Kisacası IP verilerin internetteki iletiminin kalbini oluşturan protokoldür. IP paketi çalıştırılarak oluşturulmaktadır. Paketin en başında bir paket başlığı vardır ve gönderilecek olan veriyle ilgili olarak gideceği adres, gönderen adres gibi bilgileri içermektedir. Paketin geri kalan kısmı ise gönderilecek veriyi içerir. IP paketleriyle ilgili en ilginç şey bu paketler yolculuğu sırasında daha ufak paket boyutları kullanan ağlara rast geldiklerinde daha küçük parçalara bölünmesi ve karşı tarafta tekrar birleştirilmesidir.

IP protokolü ile ilgili daha fazla bilgi RFC 760 dokümanından edinilebilir.

Transfer kontrol protokolü: TCP protokolü; internette kullanılan ana protokoldür. Dosya transferi ve uzak oturumlar gibi kritik işleri sağlar. TCP diğer protokollerden farklıdır. Güvenli bir iletişim ortamında verilerin aynı şekilde hedefe ulaşacağından emin olamazsınız. Ancak TCP gönderilen verilerin gönderildiği sırayla karşı tarafa ulaşmasını sağlayarak güvenli veri iletimini sağlar. TCP iki makine arasında kurulan sanal bir bağlantı üzerinden çalışır. Çalışması; kısmi bir işlemde oluşur bu bağlantı ve three-part handshake olarak bilinir. (TCP/IP three way handshake) TCP/IP üzerinde yapılan bazı saldırı tekniklerini iyi anlayabilmek için TCP'nin çalışmasını iyi anlamak gerekmektedir. Bu nedenle şimdi bu bağlantının nasıl olduğuna bir bakalım:

Three-way handshake işleminde öncelikle istemci sunucuya port numarasıyla birlikte bir bağlantı isteği gönderir. İsteği alan sunucu bu isteğe bir onay gönderir. En sonunda da istemci makine sunucuya bir onay gönderir ve bağlantı sağlanmış olur. Bağlantı yapıldıktan sonra veri akışı her iki yönde de yapılabilmektedir. Buna genellikle full-duplex iletişim denmektedir.

TCP aynı zamanda hata kontrol mekanizması da sağlıyor. Gönderilen her veri bloğu için bir numara atanmaktadır. Ve karşılıklı iki makine de bu numarayı kullanarak transfer edilen blokları tanımlıyorlar. Başarılı olarak gönderilen her blok için

alici makine gönderici makineye bir onay mesajı gönderir. Ancak transfer sırasında hata olursa alıcı makine ya hata mesajları alır ya da hiçç bir mesaj almaz. Hata olustugu durumlarda, oturum kapanmadığı sürece, veriler tekrar gönderilir. TCP protokolü ile verinin iki makine arasında nasıl transfer edildiğini gördük. Simdi istemcinin isteginin karşı tarafa ulaştığında ne olup bittiğine bakalım. Bir makine başka bir makineye bağlantı istediği zaman belli bir hedef adresi belirtir. Bu adres bir IP adresi ve fiziksel adrestir. Ancak sadece bu adres te yeterli değildir, istemci karşı makinede hangi uygulamayla konuşmak istediğini de belirtmek durumundadır. &Ouml;rnek olarak siz bir sayfaya bağlanmak istediğinizde URL adres kısmına www.guvenlikhaber.com adresini yazıp bağlan dediginiz anda browser bu adresteki bilgisayara bir bağlantı istediği gönderir ve o makinede bulunan HTTP uygulamasıyla konuşmak istediğini de belirtir. Simdi bu HTTP isteginizin karşı tarafa gittiği zaman neler olduğuna bakalım.

## inetd

inetd tüm daemon'ların anasıdır. Daemon'lar sistemde devamlı olarak &ccedil;alisan ve diğer prosesleri dinleyen programlardır. Microsoft DOS platformundaki terminate and stay resident TSR programlarına benzerler. (TSR genellikle virüsler tarafından &ccedil;ok kullanılan bir yöntemdir. Virüs kodunun sürekli hafızada aktif olarak kalabilmesi i&ccedil;in TSR metodu kullanılıyordu.) Daemonlar sistem a&ccedil;ik olduğu sürece belli bir olayı dinlemek i&ccedil;in sürekli &ccedil;alısır durumdadırlar. liste süper sunucu olarak ta &ccedil;agrılan inetd tüm bu daemonların büyük büyük babasıdır.

Tahmin edebileceğiniz gibi bir sistemde ne kadar &ccedil;ok daemon varsa o kadar &ccedil;ok sistem kaynakları azalacaktır. İşte her türlü işlemi ger&ccedil;ekleştirmek i&ccedil;in bir daemonu her zaman &ccedil;alısır durumda bekletmek ve sistem kaynaklarını yemek yerine bir tane daemon yazmışlar. Bu da inetd daemonudur. inetd tüm ağ isteklerini dinler ve bir istek geldiğinde isteğe bakarak hangi servisle ilgili olduğuna karar verir. Daha sonra da ilgili servisi sunan uygulamayı yükleyerek istediği bu uygulamaya yönlendirir. &Ouml;rnek olarak bir FTP istediği zaman inetd FTP sunucusunu başlatır ve isteğe cevap vermesini ister ve kendisi de başka isteklere cevap vermek üzere dinlemeye devam eder.

inetd sadece UNIX üzerinde &ccedil;alisan bir uygulama değildir. Windows ortamında &ccedil;alısın sürümlerini de piyasada bulmak mümkündür. Hummingbird'ün Exceed ürünü Windows ve OS/2 platformları i&ccedil;in inetd'yi sunmaktadır.

inetd programı normal olarak sistem a&ccedil;ildiğinde &ccedil;alışmaya başlar ve sistem yöneticisi tarafından kapatılmadığı sürece sistem kapatılana kadar da &ccedil;alışmaya devam eder. inetd programının &ccedil;alışması /etc/inetd.conf konfigürasyon dosyası ile tanımlanır. inetd'nin hangi servisleri sunacağı bu dosyada belirtilir. Bu servisler FTP, Telnet, SMTP, Finger, Netstat.. gibi servislerdir.

## portlar

TCP/IP ortamında programların &ccedil;alıştırılması ve servisler genellikle istemci-sunucu tabanlıdır. Her bağlantı istediği i&ccedil;in inetd bir sunucu &ccedil;alıştırır ve sunucu da istemciyle haberleşmeye başlar.

Bu işlemi ger&ccedil;ekleştirebilmek i&ccedil;in her servise (FTP, Telnet.. gibi ) bir numara verilmiştir. İşte istemciler bu numaraları kullanarak karşı bilgisayardaki hangi uygulamayla konuşacağını belirtir. Bu numaralar port numaraları olarak adlandırılır. Bir internet sunucusunda binlerce port olabilir. Ancak etkin bir kullanım i&ccedil;in iyi bilinen ve her zaman kullanılan servislere standart port numaraları verilmiştir. Sistem yöneticisi istediği servisi istediği port numarasına bağlayabilir ancak normal olarak iyi bilinen port numaraları (well-known ports) kullanmak akıllıca olacaktır. &Ouml;rnek olarak aşağıda bazı

servislerin standart port numaralari verilmistir:

Dosya Transfer Protokolü (FTP)21Telnet23Simple mail transfer protokol (SMTP)25Gopher70Finger79HTTP80NNTP119  
Tüm port numaralarini adresinden görebilirsiniz.  
Simdi kisaca bu uygulamalara bir göz atalim:

Telnet: Telnet protokolü RFC 854 dökümaninda anlatilmistir. Telnet uzak sistemlere login olmak ve sistemde komut &cedil;alistirmek i&cedil;in kullanilir. Ankarada bulunan bir kullanıcı Istanbulda bulunan bir makineye telnet yaparak sanki makinenin basındaymiş gibi komutlar &cedil;alistirabilir. Bir telnet oturumu a&cedil;mak i&cedil;in UNIX komut satirindan yada DOS komut satirindan:

```
#telnet sunucu_adi
```

komutu girilir ve eger bu sunucuda telnet sunucusu &cedil;alisiyorsa kullanıcının karsısına login ekranı gelecektir. Bu ekranda kullanıcı adı ve şifresi girildikten sonra sisteme oturum a&cedil;ilacaktır. Telnet protokolü text tabanlı olup UNIX sisteminde ve &cedil;ogu sistemde dahili olarak gelmektedir.

Dosya Transfer Protokolü: FTP protokolü RFC 0765'de tanımlanmıştır ve protokol spesifikasyonu RFC 114 dökümanında anlatılmıdır. FTP internette standart olarak dosya transferi i&cedil;in geliştirilmiş bir protokoldür. Uygun ftp istemcileri kullanılarak ftp sunucularından yararlanılabilir. UNIX ve Windows platformlarında standart komut satiri ftp istemcisinin yani sıra, Cute-FTP (Windows), FTP Explorer (Windows), FTPTool (UNIX) gibi &cedil;ncü parti ara&cedil;lari da vardır.

FTP istemcileri karşı tarafta bir FTP sunucusuyla konuşurlar. İste karşıda istemci isteklerine cevap veren standart ftp daemonu FTPD'dir. Bu daemon UNIX sistemlerinde default olarak gelmektedir. Ancak diğer sistemlerde de kullanılabilir ftp sunucuları mevcuttur. Windows'ta WFTP, Frontpage, WAR FTP Daemon, NT'de Microsoft Internet Information Server, Machintosh'ta FTPD &cedil;rneği olarak verilebilir.

Basit e-posta transfer protokolü: SMTP protokolü RFC 821 dökümanında tanımlanmıştır. SMTP protokolünün amacı etkili ve güvenli bir şekilde posta iletimini sağlamaktır. Kullanıcı SMTP destekleyen bir istemciyle SMTP sunucusuna bir istek gönderir ve iki yönü bir bağlantı kurulur. Bağlantı kurulduktan sonra eger sunucu izin veriyorsa istemci MAIL komutları göndererek posta gönderme işlemini yapabilir. (İnternette kullandığımız Netscape ve Explorer gibi browserlar genellikle SMTP sunucularını kullanarak mail gönderirler. Browser ilk kurulduğunda kullanıcı posta ayarlarında verdığımız SMTP sunucusunun adı mail göndermek i&cedil;in kullanılmaktadır) SMTP'nin bu &cedil;ok basit yapısının yani sıra bir &cedil;ok güvenlik a&cedil;isinin kaynağı olmuştur. Bunun nedeni ise SMTP'nin &cedil;ok fazla parametresinin bulunmasıdır. Yanlış konfigürasyonlar güvenlik a&cedil;ilerinin nedeni olmaktadır.  
SMTP sunucusu UNIX sistemlerinde default olarak gelmektedir.

Gopher: Gopher servisi dağıtılmış döküman paylaşım sistemidir. Dökümanlar ve servisler sunucularda saklanıyor ve Gopher istemci programı kullanıcıya bu dökümanlara bir hiyerarşik şekilde ulaşma imkanı sunuyor. Dosya ve izin yapısı dökümanları yerleştirme ve kullanma i&cedil;in uygun olduğu

içinde daha çok bu yapıya benzetilerek tasarlanmış Gopher.  
Gopher'in akil almaz gelişimi ve kullanım yaygınlığı nedeniyle  
bu servis artık kullanılmaz hale gelmiştir. Gopher ile ilgili ayrıntılı bilgi RFC 1436  
dokümanından edinilebilir.

**Hipertext transfer protokolü:** İnternette kullanıcıların srf yapmasını sağlayan  
HTTP herhalde tüm protokoller içinde en hızlıdır.  
HTTP protokolü RFC 1945 ve RFC 2068 dokümanında anlatılmıştır.  
HTTP protokolü; internetin kullanımını tamamen değiştiren ve herkes tarafından  
kullanılabilir bir hale getirmiştir. HTTP protokolü de Gopher mantığıyla çalışır.  
İstem ve cevap şeklinde bir çalışır. Telnet gibi uygulamalar istemcinin  
login olmasını ve işlemler devam ettiği sürece de bağlı kalmasını gerektirmektedir.  
Ancak Gopher ve HTTP'de böyle bir zorunluluk yoktur. İstemci istediği zaman istediği  
istegi gönderir ve sunucuda bu isteğe cevap verir. Bunu internet browserdan  
görmek mümkündür. Siz bir adresi ziyaret ederken aslında o siteye  
bağlı değilsinizdir o siteden bazı dokümanlar indirmiş ve bunları yerel olarak  
görmüyorsunuzdur. Ancak bir linke tıkladığınızda o sunucuyla bağlantı kurulur ve  
bilgiler transfer edilir bu işlemin işleyişini ekrandaki durum üzerinden  
görebilirsiniz.

Tabii HTTP sunucularına bağlanmak için HTTP protokolü; &ouml;grenip  
bir istemci programı yazmadığınız sürece &ouml;&ouml;nc&ouml; parti bir  
HTTP istemcisi kullanmak zorundasınız. Bunların arasında Windows için, Netscape,  
Microsoft İnterent Explorer, Opera, Mosaic, WebSurfer, UNIX için Xmosaic, Netscape,  
Lynx, Arena, OS/2 için Web Explorer, Netscape sayılabilir.

HTTP sunucusu artık hemen hemen tüm işletim sistemlerinde mevcuttur. Kisisel HTTP  
sunucularından kurumsal sunuculara kadar geniş bir yelpazede &ouml;r&ouml;nler ortaya  
çıkmiştir. &ouml;rnek olarak, Windows için OmniHTTPD, Microsoft Personal  
Web Server, Website, Windows NT için HTTPS, IIS, Alibaba, Espanade, Espresso,  
UNIX için HTTPD, Apache, OS/2 için GoServe, OS2HTTPD, IBM İnternet  
Connection Server verilebilir.

**Network News transfer protokolü :** NNTP en çok kullanılan protokollerden  
biridir. USENET olarak bilinen haber servisine erişim sağlar. NNTP RFC 977  
dokümanında tanımlanmıştır. NNTP protokolü; &ouml;&ouml;n çalışması  
SMTP protokolüne benzer, sunucuya gönderilen komutlar anlaşılabilir bir  
şekildedir.

Şimdi artık TCP/IP servis ve protokol ailesini &ouml;grendik ve aynı zamanda bazı uygulama  
dokümanı protokolleri inceledik. Burada değindigimiz protokoller internette sıklıkla  
kullanılan protokollerdir. Ancak gerçekte bunlar buzdagının görünmeyen  
parçasıdır sadece, burada değinmediğimiz daha yüzyüzerce protokol mevcuttur.

Kısaca TCP/IP tek basına interneti oluşturan bir yapıdır ve &ouml;ogu kullanıcıya  
görünmeyem protokoller topluluğudur. Şimdi standart bir internet sunucusunda  
bulunan protokolleri sıralayalım:

- Transfer kontrol protokolü; (TCP),
- İnternet protokolü; (IP),
- İnternet mesaj kontrol protokolü; (ICMP),
- Adres çalışır; &ouml;z&ouml;mleme protokolü; (ARP),
- Dosya transfer protokolü; (FTP),
- Telnet protokolü;,
- NNTP protokolü;,

- SMTP protokolü;
- HTTP protokolü;

Burada verilen protokoller aslında bazen birbiriyle ilişkili girmiş durumdadır. Yani internette bir noktadan bir noktaya veri transferi için bir tek yol değil bir çok yol vardır. Örnek olarak bir dosya transfer işlemini için FTP protokolünü kullanabilirsiniz. Ancak bunun için eposta (SMTP protokolü), HTTP protokolü gibi diğer yolları da kullanabilirsiniz.

### 3.3- TCP/IP ile Otel Telefon Sistemi arasındaki ilişki yeni

Fazla teknik bilmeyen ya da teknigi anlamak istemeyenler için ConSeal PC Firewall yardımcı dosyasından derlediğim TCP/IP açıklamasını sunmak istedim. ConSeal TCP/IP'yi bir benzetmeyle çok güzel bir şekilde anlatmış.

**Not:** ConSeal yardımcı; bu konuyu anlatırken konuyu reklam amacıyla kullanmış ve kendi firewall yardımcı; özelliklerini vurgulamış. Ben bu reklam kısımlarını eleyerek genel olarak anlatmaya çalıştım.

TCP/IP'yi bir telefon ağına benzetebiliriz. Bu benzetmede benzetilen terimleri listeleyelim öncelikle:

Bilgisayar sistemi Otel (müşahideler ve müşteriler için telefon sistemi için) TCP/IP kişi arasındaki telefon görüşmesi UDP Sesli mesaj bırakma işlemi Port Dahili telefon numarası Adres Otelin telefon numarası Connection Bir telefon görüşmesi Firewall Otelin telefon operatörü ARP Bir cadde adresinin bulunması Bir bilgisayar sistemini bir otelin telefon sistemine benzetebiliriz zira bilgisayar sistemi çalıştırdığınız uygulamaları barındırır. Bilgisayar sistemine firewall kurmak, otelin telefon operatörüne telefonlara ve mesajlara hangi durumlarda izin vereceğini söylemeye benzer. Bilgisayar kullanıcıları olan siz de otel yöneticisi ve VIP müşterisi olabilirsiniz.

#### Kavram 1 : Uygulamalar ve Servisler

Oteller müşterilere sahiptir ve bu müşterilerine hizmet vermek için müşterileri vardır.

Bilgisayarlar email, web browser gibi uygulamalara sahiptir ve bu uygulamaları desteklemek için DNS, RIP gibi işletim sistemi servislerini kullanırlar.

#### Kavram 2: İletişim

Otelden bir müşteri dışarıyı aramak istiyor. Oteldeki bir telefondan başka oteldeki bir telefonu arayarak o otelde görüşmek istediği kişinin dahili numarasını arıyor.

Bilgisayar da ise bir uygulama ya da bir servis başka bir bilgisayardaki bir uygulama ya da servisle konuşmak istiyor. TCP/IP ve UDP/IP kullanılarak karşı bilgisayarın IP numarasını ve port numarasını kullanarak istediği uygulamayla ya da servisle konuşabilir.

#### Kavram 3: Firewall Olmadan

Operatör olmadan herhangi bir kişi dışarıyı ya da dışarıyı arayabilir. Ve bu aradıkları dahili numarada hiç kimse olmayabilir ya da kişi telefona cevap verebilir

yada vermeyebilir.

Bilgisayar sisteminde firewall olmadan i&ccedil;eri ve disari olan t&uuml;m iletisim iletisim a&ccedil;ik durumdadir. Ancak t&uuml;m portlar kendilerini kullanan bir servise bagli olmayabilirler. Yada bir uygulama bir baglanti istegini kabul edebilir yada etmeyebilir.

**Kavram 4: Firewall'un g&ouml;revi**

Operat&ouml;r &ccedil;alistigi zaman, hangi dahili numaralarin g&ouml;r&uuml;sme yapabilecegine yada hangi otelin ve dahili numaranin aranabilecegine karar verebilir.

Bilgisayar sisteminde bir firewall &ccedil;alistigi zaman, hangi sistemlerin haberlesebilecegi ve hangi port numaralarin kullanilabilecegini belirler.

**Kavram 5: Diger PC tabanlı Firewall'lar**

Eski operat&ouml;rler bazi &ouml;nemli otel personelinin g&ouml;r&uuml;smelerini engelleyemezler. Sizin oteliniz t&uuml;m g&ouml;r&uuml;smeleri engelleyebilecek bir operat&ouml;re sahip.

Bilgisayar sisteminde Winsock tabanlı firewall'lar dosya paylasimi gibi bazi &ouml;nemli Windows servisleri i&ccedil;in bloklama yapamazlar. Ancak t&uuml;m veri paketlerini yakalayan bir firewall bu servisleri de engelleyebilir.

**Kavram 6: Diger protokoller (IPX, NetBEUI...)**

Eski operat&ouml;rler otelin bir fax makinesi yada Morse Kodu oldugunu bilmezler ve dolayisiyla bunlara erisimi engelleyemezler. Ancak sizin otelinizdeki operat&ouml;r fax makinesi ve morse kodu oldugunu biliyor. Ilerleyen zamanda operat&ouml;re bu servislerin nasil kullanilacagi &ouml;gretilecek. Ancak simdilik sadece operat&ouml;re bu servislerin kullanilip yada kullanilmayacagi &ouml;gretilmektedir.

T&uuml;m veri paketlerini yakalamayan firewall'lar IPX, NetBEUI paketlerini de yakalayamazlar ve dolayisiyla bu servisleri engelleyemezler. Ancak t&uuml;m paketleri yakalayan bir firewall bu protokolleri de yakalar.

**Kavram 7: Gelen TCP/IP baglantilarini engellemek**

Bir operat&ouml;r otelde kalan bir kisiye gelen telefon g&ouml;r&uuml;smelerine izin vermeyebilir ancak bu kisinin disariyi aramasina ve g&ouml;r&uuml;smeye yapmasina izin verebilir.

Bilgisayarda bir firewall herhangi bir TCP/IP portuna disardan gelen baglanti isteklerini engelleyebilir ancak ayni port &uuml;zerinden disari &ccedil;ikislara izin verebilir.

**Kavram 8: Paket filtreleyici firewall**

Operat&ouml;r bir aramayi engelleyebilir ancak ne s&ouml;yendigini sans&uuml;rleyemez. Bunun i&ccedil;in g&uuml;venlik g&ouml;revlisi ise yarayabilir.

Paket filtreleme yapan bir firewall iletisimi engelleyebilir ancak paketlerin i&ccedil;erigini incelemeyebilir. bunun i&ccedil;in Anti-vir&uuml;s yazilimlari ise yarayabilir.

**Kavram 9: UDP/IP ve TCP/IP karsilastirmasi**

Bazi insanlar devamlı olarak y&uuml;z y&uuml;ze g&ouml;r&uuml;smeye yaparlar, bazilari ise mesaj birakirlar. Karsilikli konusurken s&ouml;yediginiz her sey in karsidaki kisi tarafından duyulduğunu bilirsiniz ancak mesaj biraktiginiz zaman biraktiginiz mesajın karsidaki kisiye ulasip ulasmadigindan hi&ccedil; bir zaman emin olamazsiniz.

Uygulamalar tek bir datagram g&ouml;ndermek i&ccedil;in ya TCP/IP'yi ya da UDP/IP'yi kullanirlar. UDP/IP protokol&uuml; ile karsi uygulamanın iletii alip almadigindan hi&ccedil; bir zaman emin olamazsiniz.

**Kavram 10: UDP/IP verisini engelleme**

Eger otel operat&ouml;r&uuml; bir m&uuml;sterinin baska bir oteldeki bir kisiye mesaj

birakmasına izin veriyorsa, bu diğer oteldeki kişinin de bu mesaj bırakmasına izin verecektir.

Eğer firewall uygulamalara ve servislere UDP/IP üzerinden ve belli portları kullanarak diğer sistemlere bilgi göndermesine izin verecek bir kurala sahipse, diğer sistem de aynı portları kullanarak size veri gönderebilir. Bunun nedeni karsındaki sistemin size ilk kez veri mi gönderdiği yada cevap mı verdiği tam olarak bilinmiyor olmasıdır.

#### Kavram 11: Portlar nasıl kullanılıyor (1)

Lobide bulunan telefon her kes tarafından dışarıya telefon etmek için hazırdır. Genel olarak otel çalışanlarına ve servislerine ait dahili numaralar 1 ile 1023 arasındadır.

Diğer dahili numaralar ise 1024 ve 5000 arasındadır.

Uygulamaların diğer sistemlerdeki servislerle konuşabilmeleri için belli bir port aralığı mevcuttur. Genel olarak servisler 1 ile 1023 port numaraları arasında yer almaktadır.

Geçici olarak kullanılacak port numaraları ise 1024 ve 5000 arasındadır. Böylelikle uygulama yada servislere sistem servislerinin port numaraları verilmez.

#### Kavram 12: Portlar nasıl kullanılıyor (2)

Bir gelenek olarak otellerde bulunan belli başlı servisler sabit bir dahili numaraya sahiptir. Örneğin olarak salonun dahili numarası 80, Bellman için dahili numara 23 gibi.

Böylelikle misafirler diğer otellerdeki çalışanlara hangi numaradan erişeceklerini her zaman bilirler. Aynı zamanda müşterilerden bu dahili numaraları kişisel görüşmeler için kullanmamaları istenir.

TCP/IP'de ve UDP/IP'de bir gelenek olarak belli başlı bazı servisler her sistemde hep aynı port numarasında bulunur. Örneğin olarak Web sunucusu 80 numaralı portta, DNS servisi 53 numaralı portta, telnet 23 numaralı portta bulunur. Bu şekilde sizin uygulamanız diğer sistemlerdeki servislere nasıl erişeceğini biliyor. Uygulamalar bu port numaralarını uygunsuz olarak kullanmamalıdır.

#### Kavram 13: Kural kullanımı

Otel bazı görüşmelere bazı özel durumlarda izin verip vermemeye karar verebilecek bir operatöre sahiptir. Bu durumlar örnek olarak şöyle olabilir: sadece belli bir müşteri oteldeyse izin verebilir yada görüşme otelin görüşmeli görüşme hattından yapılacaksa izin verilebilir.

Firewall ile belli kurallar koyarak iletişime belli durumlarda izin verip belli durumlarda izin vermeyebilirsiniz. Örneğin olarak belli uygulamalar çalışıyorsa, evirmeli bağlantı aktif ise yada iletişim görüşmeli bir VPN (sanal ağ) bağlantısı üzerinden yapılıyorsa izin verilebilir.

#### Kavram 14: Kuralların öncelik sırası

Otel operatörü için bazı talimatlar diğerlerine göre daha önemlidir. Her bir kural için bir önem derecesi belirleyerek operatörün bu sıraya uymasını sağlayabilirsiniz.

Firewall kural setinde bazı kurallar diğer kurallara göre önceliğe sahiptir. Bu önem derecesini ayarlayarak (default olarak 100'den) kuralların uygulanma sırasını ayarlayabilirsiniz. Küçük numaralar öncelik hakkına sahiptirler ve ilk olarak test edilirler.

#### Kavram 15: Paranoya ve bilgi savaş oyunu

Oteliniz diğer otellerle aynı blokta yer alıyor. Önemli bir ayrıntı eğer otelin bulunduğu caddeyi bilmeden otelle görüşme yapamıyorsunuz. Otel çalışanları da kolayca bu bilgileri unutabiliyorlar ve her bir kaç dakikada bir birbirlerine otel adresini soruyorlar. Eğer operatör otel çalışanlarının bu bilgi alışverişini engellerse insanlar hiç konuşamayacaklardır.

Sizin bilgisayarınız diğer sistemlerle aynı ağda bulunuyor. Önemli bir ayrıntı diğer bilgisayarların Ethernet Adresini bilmeden (ARP protokolü ile elde ediliyor) bilgi alıs verisinde bulunamıyorsunuz. Sizin bilgisayarınız bu bilgiyi eğer devamlı olarak kullanılmıyorsa siliyor kayıtlarından dolayısıyla haberleşmek istediği zaman diğerlerine bu adresi soruyor her seferinde. Eğer ARP'yi engellerseniz sistemler hiç bir zaman konuşamayacaklardır.

Bundan sonraki kavramlar neden firewall kullanmanız gerektiğini açıklayacak ve özellikle ilgili kavramlardır.

#### Kavram 16: IRC ve Nukeleme

Telefonda sohbet eden insanlar diğer otellerdeki kişilerin araya girip kesinti yapmalarına davetiye çıkarıyor. Bu mesajlar sizin otel resepsiyonunuza bağlantıyı kesmesini sağlar. Resepsiyon da nedensiz bir şekilde kesiyor bağlantıyı. Bunu engelleyecek bir operatör olmazsa mesajlar durumdan geçerken okutulurlar.

Sohbet gruplarını kullanan insanlar kötü niyetli kişilere can sıkıntısı yapmak için davetiye çıkarıyorlar. Bu lamer'lar sisteminize ICMP nuke ve diğer datagramlar göndererek chat sunucusuna erişmesini engelleyebilir. Bunu engelleyecek bir Firewall yoksa Windows sisteminde IRC chat geçerken can sıkıcı olabilir. Tabii ki firewall'lar ICMP'yi engelleyemeyebilir.

#### Kavram 17: Gizlice dinleme

Sizin otel mesajlaşmalarınız ve mesajlarınız başka bir oteldeki bir kişiye gönderilirse yapıyorsa bile başka otellerdeki insanlar bu konuşmaları dinleyebilir. Sizin bilgisayarınız başka bir bilgisayarla haberleşirken, paylaşımlı bir ağ üzerinden konuştuğu diğerleri de sinsice sizin konuşmalarınızı dinleyebilir. (bildiğimiz gibi bu cihazlar sniffer'lardır.)

#### Kavram 18: Onaylama

Mesela bir yerde bulunan insanlar operatör; başka bir yerden arıyormuş gibi kandırabilir ve gönderilmesini izni alabilir. Bu durumda arayanı tanımak aranan kişiye kalıyor.

Bilgisayarlar da kendi IP adreslerini değiştirerek gönderilen bir sistemmiş gibi davranabilir. Bu durumda bu sistemi tanıma ve onaylama işi uygulamaya kalıyor.

#### Kavram 19: TCP bağlantı hırsızlığı

İki kişi telefon konuşması yaparken mesaj; bir kişi araya girip konuşmayı keserek bir kişinin yerini alabilir ve diğer kişiye karşı yerini aldığı kişiyim gibi konuşmaya devam edebilir. Güvenli bir telefon hattı olmaksızın bunun olup olmadığını hiç bir zaman anlamayabilirsiniz.

Bir hacker için bir TCP bağlantısını kesip iletişimde bulunan sistemlerden birinin yerine geçebilir. VPN gibi güvenli bir bağlantı olmaksızın sisteminiz bunu hiç bir zaman anlayamayacaktır.

#### Kavram 20: DNS Spoofing

Eğer bir kişi Directory Asistanı (411) (bizde bilinmeyen numaralar 118 olarak dışarı verilir) gibi davranırsa numara isteyen kişilere yanlış numaralar vererek başka kişilerle konuşmanızı sağlayabilir.

Eğer bir hacker bir DNS (alan adı sunucusu) sunucusunun yerine geçerse, size yanlış IP numaraları sağlayarak sisteminizin istemediğiniz başka bir bilgisayarla konuşmasını sağlayabilir.

### **Kavram 21: Verinin degistirilmesi**

Eger bir kisi sizin konusmaniza girmeyi basarsa s&ouml;ylenilen seyleri degistirebilirler. G&uuml;venli bir telefon hattı bu sorunu &ccedil;&ouml;zer.

Eger bir hacker iletisiminizi kesip araya girebilirse g&ouml;nderilen veriyi degistirebilirler. VPN gibi g&uuml;venli iletisim saglayan baglantilar bu sorunu &ccedil;&ouml;zebilir.

### **Kavram 22: Verinin ele ge&ccedil;irilmesi (1)**

Otel telefon sistemlerinin bir sasirtici &ouml;zelligi bir noktadan diger bir noktaya ulasincaya kadar telefon g&ouml;r&uuml;smesi otelden otele gezmektedir. Iste bu sirada bir &ccedil;ok kisi sizin g&ouml;r&uuml;smenizi dinleyebilir. Bu y&uuml;zden ne s&ouml;ylediginize dikkat etmelisiniz yada g&uuml;venli bir hat kullanmalisiniz.

Internetin &ouml;nemli bir &ouml;zelligi ise veriler belli bir hedefe giderken bir &ccedil;ok bilgisayar gezerler. Bunun anlami bir &ccedil;ok kisi sizin g&ouml;nderdiginiz bilgileri izleyebilir ve ele ge&ccedil;irebilir. Bu y&uuml;zden ne g&ouml;nderdiginize dikkat etmelisiniz yada VPN baglantisini kullanmalisiniz.

### **Kavram 23: Verinin ele ge&ccedil;irilmesi (2)**

Oteller arasindaki bazi linkler mikrodalga baglantilar &uuml;zerinden radyo yayini seklinde olmaktadır.

Bazi telefon g&ouml;r&uuml;smeleri mikrodalga anahtarlarindan y&ouml;nlendirilmektedir ve cep telefonlari en yakin istasyona yayin yapmaktadır. Bu verinin daha fazla erisilebilir bir konumda olmasini saglamaktadır.

### **Kavram 24: Ag g&uuml;venligi**

Bir oteldeki m&uuml;steriler otelin isini &ccedil;ok iyi yapan bir operat&ouml;rre sahip oldugunu bildikleri i&ccedil;in &ccedil;ok rahat bir sekilde uyuyabilirler, baska bir oteldeki m&uuml;steriler de otellerine g&ouml;r&uuml;smeleri kontrol ltina alacak bir operat&ouml;r&uuml;n geldigini bilerek rahat olabilirler. (Biraz karmasik gibi gelebilir bunu anlamasi. Ancak konunun asagidaki bilgisayar d&uuml;nyasindaki karsiligina baktiginizda daha rahat anlayacaksınız.)

Mac sistemleri ag g&uuml;venligi konusunda &ccedil;ok iyi bir &uuml;ne sahiptirler. Ancak kisisel firewall yazilimlari ile artik Windows kullanicilari da rahat bir nefes alabilirler.

Bu d&ouml;k&uuml;man artiiisttarafindan eklenmistir.

[www.mircla.com](http://www.mircla.com) Turkce Mirc Sitesi